UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/724,034	11/26/2003	Markus Jakobsson	1048-008	7279

80360 7590 07/09/2008

Bainwood, Huang & Associates, LLC
2 Connector Road
Westborough, MA 01581

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	PAPER NUMBER
2132	
MAIL DATE	DELIVERY MODE
07/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/724,034	JAKOBSSON ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-14 and 16-87* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *2-4,6-10,12,14,16-25,73-75 and 77-82* is/are allowed.

6)☒ Claim(s) *5,11,13,26-32,35-59,65-72,76 and 83-87* is/are rejected.

7)☒ Claim(s) *13,33-34,60-64* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in reply to amendment after a non-final office action, filed on March 12, 2008. Claim 1 and 15 are canceled. New claims 86-87 are added, thus claims 2-14, 16-87 are pending/ examined.

2. The amendment made to claims 2 and 73 overcomes the 112 rejection set forth in the pervious office action, Thus the 112 rejection is overcome.

Priority

3. This application claims priority of a provisional application, application No. 60/429754 filed on November 27, 2002. Therefore, the effective filling data for the subject matter defined in the pending claims of this application is 11/27/2002.

Response to Arguments

4. Applicant's argument filed on March 12, 2008 has been fully considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty

defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 26-32 , 35-56 and 87 are rejected are rejected under 35 U.S.C. 102(e) as being anticipated by Allahwerdi et al (Hereinafter referred as Allahwerdi) (U.S. Patent No. 6,928,558) filed on Oct. 27, 2000)

7. **As per independent claims 26 Allawerdi discloses a method for generating an identity authentication code** *[See, column 7, lines 36-37, "one time password"]* **associated with an authentication device,** *["mobile station"/***comprising the steps of:**

- **Providing event state data that is a security indicator for an authentication system of which the authentication device is a component***[IMEI device-specific identifier on column 7, lines 25-35"]* ; **and**
- **Generating an identity authentication code** *[see column 7, lines 36-37, "one time password"]* **that depends at least in part on (i) the event state data,** *[IMEI device-specific identifier on column 7, lines 25-35"]* **and (ii) a secret associated with the device. [***See "a subscriber-specific identifier A_SCRBR, column 7, lines 35 or the "pin"].*

8. **As per independent claims 43 Allawerdi discloses a method for generating an identity authentication code** *[See, column 7, lines 36-37, "one time password"]* **associated with an authentication device,** *["mobile station"/***comprising the steps of:**

- **Providing event state data that specifies information about a user of the authentication device** *[See on column 7, lines 35 "pin"]* ; **and**

- **Generating an identity authentication code** *[see column 7, lines 36-37, "one time password"]* **that depends at least in part on (i) the event state data,** *["pin" on column 7, lines 25-35"]* **and (ii) a secret associated with the device. [***See "a subscriber-specific identifier A_SCRBR, column 7, lines 35 or IMEI device-specific identifier on column 7, lines 25-35"]"*

9. As per dependent claim 27-28, 44-45 Allawerdi discloses a method as applied to claims above. Furthermore Allawerdi discloses the method wherein the identity authentication code further depends on a dynamic value.[See "time" on column 7, line 36]

10. As per dependent claim 29-32, 35-42, 46-56 and 87 Allawerdi discloses a method as applied to claims above. Furthermore Allawerdi discloses the method, wherein the identity authentication code further depends on one or more of a PIN, a password, data derived from a biometric observation, user data, verifier data, and a generation value.[See column 7, lines 33-34; see also column 6-7]

11. **Independent Claim 57** is rejected under 35 U.S.C. 102(b) as being anticipated by **Olarig et al** (Hereinafter referred as **Olarig)** (U.S. Patent No. 6,032,257), Patent Date: 02/29/2000)

12. **As per independent claim 57, Olarig** discloses a method of generating an identity authentication code associated with an authentication device,[See authentication code on column 6, line 11] comprising: providing event state data that specifies information about environmental conditions associated with the authentication device [See the site code on column 6, line 11; and,

generating an identity authentication code [See authentication code on column 6, line 11] that depends on (i) the event state data, [See the site code on column 6, line 11 and (ii) a secret associated with the device [See device serial number on column 6, lines 11]

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. **Claims 5, 11, 86** are rejected are rejected under 35 U.S.C. 103(a) as being unpatentable over **Allahwerdi et al** (Hereinafter referred as **Allahwerdi)** (U.S. Patent No. 6,928,558) filed on Oct. 27, 2000 in view of **Smithies et al** (Hereinafter referred as **Smithies)** (U.S. Patent No. 6,091,835), Patent Date: 07/18/2000)

15. As per dependent claims 5 , 11 and 86 Allawerdi discloses a method for generating an identity authentication code *[See, column 7, lines 36-37, "one time password"]* **associated with an authentication device,** *["mobile station"/***comprising the steps of:**

- **Providing event state data that is a security indicator for an authentication system of which the authentication device is a component***[IMEI device-specific identifier on column 7, lines 25-35"]* ; **and**
- **Generating an identity authentication code** *[see column 7, lines 36-37, "one time password"]* **that depends at least in part on (i) the**

event state data, *[IMEI device-specific identifier on column 7, lines 25-35"]* **and (ii) a secret associated with the device. [***See "a subscriber-specific identifier A_SCRBR, column 7, lines 35 or the "pin"].*

Allahwerdi does not explicitly discloses

- wherein the condition of the authentication device includes information about whether the device has been subjected to tampering.

However, in the field of endeavor **Smithies discloses,** the condition of the authentication device includes information about whether the device has been subjected to tampering. [See column 14]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of having a response to the event state like tampering as per teachings Smithies in to the method of as taught by **Secure Computing** for the purpose strengthening the authentication process and the integrity of the system. [See column 14, Smithies]

16. **Dependent Claims 58-59 and 65-72** are rejected are rejected under 35 U.S.C. 103(a) as being unpatentable over **Olarig et al** (Hereinafter referred as **Olarig)** (U.S. Patent No. 6,032,257), Patent Date: 02/29/2000) in view of **Allahwerdi et al** (Hereinafter referred as **Allahwerdi)** (U.S. Patent No. 6,928,558) filed on Oct. 27, 2000

17. **As per dependent claim 58-59 and 65-72, Olarig** discloses a method of generating an identity authentication code associated with an authentication device,[See authentication code on column 6, line 11] comprising:

providing event state data that specifies information about environmental conditions associated with the authentication device [See the site code on column 6, line 11; and,

generating an identity authentication code [See authentication code on column 6, line 11] that depends on (i) the event state data, [See the site code on column 6, line 11 and (ii) a secret associated with the device [See device serial number on column 6, lines 11]

Olarig does not explicitly discloses

Wherein the identity code further depends on a dynamic value

wherein the identity authentication code further depends on one or more of a PIN, a password, data derived from a biometric observation, user data, verifier data, and a generation value,

However, in the field of endeavor **Allawerdi discloses** the method

wherein the identity authentication code further depends on a dynamic value.[See "time" on column 7, line 36]

a method for generating an identity authentication code *[See, column 7, lines 36-37, "one time password"]* **associated with an authentication device,** *["mobile station"/*__comprising the steps of:__

- **Providing event state data that specifies information about a user of the authentication device** *[See on column 7, lines 35 "pin"]* ; **and**
- **Generating an identity authentication code** *[see column 7, lines 36-37, "one time password"]* **that depends at least in part on (i) the event state data,** *["pin" on column 7, lines 25-35"]* **and (ii) a secret associated with the device. [***See "a subscriber-specific identifier*

A_SCRBR, column 7, lines 35 or IMEI device-specific identifier on column 7, lines 25-35"]"

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features such as the method wherein the identity authentication code further depends on a dynamic value and the identity authentication code further depends on one or more of a PIN, a password, data derived from a biometric observation, user data, verifier data, and a generation value as per teachings of taught **Allawerdi into the method taught** by **Olarig** for the purpose strengthening the authentication process and the integrity of the system.

18. **Claims 83-85 and dependent claim 76** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Smithies et al** (Hereinafter referred as **Smithies)** (U.S. Patent No. 6,091,835), Patent Date: 07/18/2000) **in view of Olarig et al** (Hereinafter referred as **Olarig)** (U.S. Patent No. 6,032,257), Patent Date: 02/29/2000)

19. **As per claims 83-85 and dependent claim 76 Smithies discloses a method for verifying the correctness of an identity authentication code,**

comprising:

- **Receiving authentication information including the identity authentication code generated by an authentication device that depends on (i) a secret associated with the device, and (ii) event state data that specifies a condition of the authentication**

device;[See claims 1 and 58] *(Claim 1 recites the following which meets the limitation of the above recitation, "a computer system for creating a secure, tamper-resistant electronic transcript which memorializes the events of a user's affirmation, through the entry of a signature token, of an electronic transaction having terms, the system comprising: a. a transaction application module enabling an affirming party to create an electronic transaction; b. a transcript generator module; and c. a signature token verification module accepting the signature token from the affirming party." Furthermore claim 58 discloses the following which also meets the above recitation, "a computer based system for recording a series of acts constituting the signing of an electronic document and assuring an affirming party's intent, comprising: presentation means presenting an electronic document to be signed to the affirming party, the presentation means allowing the affirming party to electronically examine the document by accepting an at least one document review affirming party input command and displaying an at least one portion of the document in accordance with the at least one document review affirming party input command, the presentation means displaying a declaration of intention indicating the intention of the affirming party towards the document; verification means verifying the identity of the affirming party by requesting identity information from the affirming party and accepting identity information from the affirming party; checksumming means creating a document checksum of the document;ceremony generating means generating ceremony information from: the presentation of the document to the affirming party; the at least one document review*

affirming party input command and the at least one portion of the document displayed)

- **Verifying the correctness of the identity authentication code, and determining the condition of the authentication device in response to the received identity authentication code.** [See claims 1 and 58] *(Claim 1 recites the following which meets the limitation of the above recitation, "a signature token verification module accepting the signature token from the affirming party, verifying the signature token and transmitting a verification signal to the transcript generator module; wherein the transcript generator module accepts the terms, confirms the acceptance of the terms by presenting prompts, allows the affirming party to affirm the terms, gathers forensic data surrounding the affirming party's affirmation and stores information related to the prompts, the forensic data and the verified token as separate data entities in a tamper-resistant transcript object." Furthermore, claim 58 discloses the following which also meets the above recitation, "verification means verifying the identity of the affirming party by requesting identity information from the affirming party and accepting identity information from the affirming party; checksumming means creating a document checksum of the document; ceremony generating means generating ceremony information from: the presentation of the document to the affirming party; the at least one document review affirming party input command and the at least one portion of the document displayed; and the at least one identity input event relating to*

the identity information; and storing the identity information, document checksum and ceremony information in a transcript object.")

Smithies does not explicitly discloses

event state data representing an occurrence of a reportable event concerning a condition of the authentication device; and/or providing event state data that is a security indicator for an authentication system of which the authentication device is a component or providing event state data that specifies information about the user of the authentication device or information about environmental condition associated with the authentication device.

However, in the field of endeavor Olarig discloses a method of generating an identity authentication code associated with an authentication device,[See authentication code on column 6, line 11] comprising:

providing event state data that specifies information about environmental conditions associated with the authentication device [See the site code on column 6, line 11; and,

generating an identity authentication code [See authentication code on column 6, line 11] that depends on (i) the event state data, [See the site code on column 6, line 11 and (ii) a secret associated with the device [See device serial number on column 6, lines 11]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features such as "*providing event state data representing an occurrence of a reportable event concerning a condition of the authentication device/* **environmental**

conditions associated with the authentication device as per teachings **Olarig** into the method of as taught by **Smithies** for providing protection of data in the authentication device and achieving confidentiality when the authentication device is tampered or stolen.

Allowable Subject Matter

20. Claims 2-4, 6-10, 12, 14,16-25, 73-75 and 77-82 are allowed.

21. Claims 13, 33-34 and 60-64 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

22. The previous prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

a. **U.S. Patent No. 5, 251,259** discloses a method for generating an identify authentication code using different event state features as it is described on figure 3 and claim 1) comprising the steps of:

- storing events in an authentication device (See for instance "frequency of use")
- modifying the event state in response to an event ("See for instance "respone") and
- generating an identify authentication code that depends on at least in part on a dynamic value (day), the event state (number of usage) and a secret (Pin) associated with authentication device. Furthermore, the method

discloses dynamic value associated with a time period or interval (See for instance, column 2)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-873-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

06/25/2008

/Samson B Lemma/

Examiner, Art Unit 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132